A – 4

An application of Max Plus Algebra in Cryptography

Musthofa
Math Education Department
Yogyakarta State University

Max plus algebra has been applied in many areas, such as transportation, manufacturing and information technology. In this paper we discuss an application of matrix over max plus algebra to build a password for keeping secret information. The algorithm used in this method adopt from Stickel's key exchange protocol.

Key Words : Max plus algebra, matrix, Stickel's key exchange protocol.

INTRODUCTION

The rapid development in information and technology force us to ensure that our information is secure. Cryptography as a way for keeping secret information has been developed by many expert. There are two famous systems in cryptography, symmetric and asymmetric cryptography.

Symmetric cryptography is a method of cryptography that use the same key in encryption and description processes. Therefore, key or password is very important in this system. All parties, who want to exchange secret information must agree on the same key. Because of the importance of the key, several methods based on group, semiring and matrix and other mathematical systems have been produced.

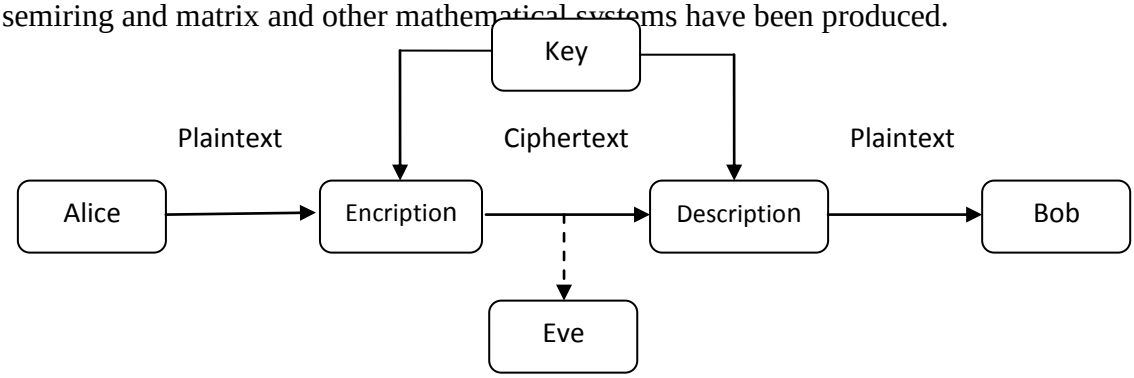

Figure 1. Symmetric Key Cryptography

In symmetric cryptography, one of the famous methods to establish the shared secret key was invented by Whitfield Diffie and Martin Hellman in 1976. The Diffie–Hellman key exchange method allows two parties to establish a shared secret key over an insecure communications channel.

Alice or Bob published finite cyclic group with generator $g \in G$.	
Alice	**Bob**
1. Alice select $a \in \mathbb{N}$	1. Bob select $b \in \mathbb{N}$
2. Alice compute g^a	2. Bob compute g^b
3. Alice send g^a to Bob	3. Bob send g^b to Alice

4. Alice receive g^b from Bob 5. Alice compute $K_A = \left(g^b\right)^a = g^{ba}$	4. Bob receive g^a from Alice 5. Bob compute $K_B = \left(g^a\right)^b = g^{ab}$
Alice and Bob have agreed on the same key $K = K_A = K_B$	

Figure 2. Diffie-Hellman Key Exchange Protocol

Following the methods, the secret key *K* has been agreed to use to perform the encryption-decryption process. On the other hand, Eve as the attacker can only determine the value of *g*, g^a and g^b. To get the key that Alice and Bob have agreed, she must determine the value of *a* or *b*. In other words, she must resolve the discrete logarithm problem in *G*, therefore the security of Diffie-Hellman key agreement protocol based on the discrete logarithm problem in the cyclic group[1].

The concept of a key agreement protocol which uses a non-commutative group has been discussed in [2]. Stickel (2005), proposed key agreement protocols based on non-commutative group. Stickel key agreement protocol scheme based on non-commutative groups as in [..] is as follows:

Let *G* be a public nonabelian finite group, $a, b \in G$ public elements such that $ab \_= ba$. The key exchange protocol goes as follows. Let *N* and *M* be the orders of *a* and *b*, respectively.

1. Alice picks two random natural numbers $n < N, m < M$ and sends $u = a^n b^m$ to Bob.
2. Bob picks two random natural numbers $r < N$, $s < M$ and sends $v = a^r b^s$ to Alice.
3. Alice computes $KA = a^n v b^m = a^{n+r} b^{m+s}$.
4. Bob computes $KB = a^r u b^s = a^{n+r} b^{m+s}$.

Thus, Alice and Bob end up with the same group element $K = KA = KB$ which can serve as the shared secret key.

DISCUSSION

An example of groups that can be applied on Stickel Key Exchange Protocol is a group of matrix multiplication over a field. Furthermore, this group can be generalized as semigroup or semiring. In this study, we apply Stickel Key Exchange Protocol on semiring : the set of all $n \times n$ matrices over the integers with the addition operation and mulitiplication defined over a max-plus algebra.

Max-Plus Algebra

Maxplus Algebra is the set $R \cup \{-\infty\}$, with *R* is the set of all real numbers completed by maximum operation($\oplus$) and addition operation($\otimes$). Moreover, ($R \cup \{-\infty\}, \oplus, \otimes$) denoted as $R_{\max}$ and $\{-\infty\}$ denoted as ε.

In $R_{\max}$, $2 \oplus 3 = 3$ and $2 \otimes 3 = 5$. Based on the algebraic structure of $R_{\max}$, It can be classified as semifield, since :

1. ($R \cup \{-\infty\}, \oplus$) is commutative semigroup

2. $(R \cup \{-\infty\}, \otimes)$ is commutative group.
3. The Operation $\oplus$ and $\otimes$ is distributive
4. The neutral element satisfying absorption property, that is
   $\forall\ a \in R_{\max}\ ,\ \varepsilon \otimes a = a \otimes \varepsilon = \varepsilon$

Matrices over $R_{\max}$

The operation of $\oplus$ and $\otimes$ on matrices over max plus algebra defined as follow: $(A \oplus B)_{ij} = A_{ij} \oplus B_{ij}$

(1) $(A \oplus B)_{ij} = A_{ij} \oplus B_{ij}$

(2) $(A \otimes B)_{ij} = \underset{k}{\oplus}(A_{ik} \otimes B_{kj})$

Example :

If $A = \begin{bmatrix} 1 & 2 \\ -2 & 3 \end{bmatrix}$ and $B = \begin{bmatrix} -2 & 7 \\ 1 & -3 \end{bmatrix}$, then

$$A \oplus B = \begin{bmatrix} 1 & 2 \\ -2 & 3 \end{bmatrix} \oplus \begin{bmatrix} -2 & 7 \\ 1 & -3 \end{bmatrix} = \begin{bmatrix} 1 \oplus -2 & 2 \oplus 7 \\ -2 \oplus 1 & 3 \oplus -3 \end{bmatrix} = \begin{bmatrix} 1 & 7 \\ 1 & 3 \end{bmatrix} \text{and}$$

$$A \otimes B = \begin{bmatrix} \{1+(-2)\} \oplus \{2+1\} & \{1+7\} \oplus \{2+(-3)\} \\ \{-2+(-2)\} \oplus \{3+1\} & \{-2+7\} \oplus \{3+(-3)\} \end{bmatrix} = \begin{bmatrix} 3 & 8 \\ 4 & 5 \end{bmatrix}$$

The power of matrix, for example A^n defined as multiplication n times of A. If $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$, then $A^3 = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 9 & 10 \\ 11 & 12 \end{bmatrix}$.

Since the multiplication is associative, then we have $A^n \otimes A^m = A^m \otimes A^n = A^{m+n}$.

Implementation on Key Exchange Protocol

Now, based on the properties of matrix operation over max plus algebra, we can construct an algorithm following the Stickel Key Exchange Protocol as below:

Alice or Bob 1 published $A, B \in (R_{max})^{n \times n}$	
Alice	**Bob**
1. Alice select two natural numbers m and n	1. Bob select two natural numbers r and s
2. Alice compute $u = A^n B^m$	2. Bob compute $v = A^r B^s$
3. Alice send u to Bob	3. Bob send v to Alice
4. Bob receive v from Alice	4. Bob receive u from Alice
5. Alice compute $K_1 = A^n v\ B^m$	5. Bob compute $K_2 = A^n u\ B^m$
Alice and Bob have agreed on the same key $K = K_1 = K_2$	

Example :

Suppose Alice or Bob published two matrices $A = \begin{bmatrix} 2 & 1 \\ 4 & 5 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 3 \\ 5 & 7 \end{bmatrix}$.

1. Alice select m = 7 and n = 4, Bob select r = 11 and s = 5.

2. Alice compute $u = A^7B^4 = \begin{bmatrix}30 & 31\\ 34 & 35\end{bmatrix}\begin{bmatrix}22 & 24\\ 26 & 28\end{bmatrix} = \begin{bmatrix}57 & 59\\ 61 & 63\end{bmatrix}$;

Bob compute $v = A^{11}B^5 = \begin{bmatrix}50 & 51\\ 54 & 55\end{bmatrix}\begin{bmatrix}29 & 31\\ 33 & 35\end{bmatrix} = \begin{bmatrix}84 & 86\\ 88 & 90\end{bmatrix}$

3. Alice send u to Bob, and Bob send v to Alice.

4. Alice compute $A^7\ v\ B^4 = A^{11}B^5 = \begin{bmatrix}147 & 149\\ 151 & 153\end{bmatrix}$; Bob compute $A^{11}\ u\ B^5 = \begin{bmatrix}147 & 149\\ 151 & 153\end{bmatrix}$.

Now, Alice and Bob have the shared secret key $K = \begin{bmatrix}147 & 149\\ 151 & 153\end{bmatrix}$.

Encryption Process

Suppose Alice want to send secret message : PLEASE GO TODAY BRO

The encryption process is as follow :

1. Break the message into blocks, each consist of 4 characters: PLEA-SEGO- TODA-YBRO

2. Convert each block into number using specific rule, for example using the table below:

0 ↔ A	1 ↔ B	2 ↔ C	3 ↔ D	4 ↔ E
5 ↔ F	6 ↔ G	7 ↔ H	8 ↔ I	9 ↔ J
10 ↔ K	11 ↔ L	12 ↔ M	13 ↔ N	14 ↔ O
15 ↔ P	16 ↔ Q	17 ↔ R	18 ↔ S	19 ↔ T
20 ↔ U	21 ↔ V	22 ↔ W	23 ↔ X	24 ↔ Y
25 ↔ Z				

Thus Alice convert the message into : 15-11-4-0; 18-4-6-14; 19-14-3-0; 24-1-17-14.

3. Convert the message into matrices :

$$p_1 = \begin{bmatrix}15 & 11\\ 4 & 0\end{bmatrix};\ p_2 = \begin{bmatrix}18 & 4\\ 6 & 14\end{bmatrix};\ p_3 = \begin{bmatrix}19 & 14\\ 3 & 0\end{bmatrix};\ p_4 = \begin{bmatrix}24 & 1\\ 17 & 14\end{bmatrix}.$$

4. Encrypt the message using the secret key K to get cipher text.

6. $(K+ p_1) \bmod 26 = \begin{bmatrix}147 & 149\\ 151 & 153\end{bmatrix} + \begin{bmatrix}15 & 11\\ 4 & 0\end{bmatrix} = \begin{bmatrix}162 & 160\\ 155 & 153\end{bmatrix} \bmod 26 = \begin{bmatrix}6 & 4\\ 25 & 23\end{bmatrix} = e_1.$

$(K + p_2) \bmod 26 = \begin{bmatrix}147 & 149\\ 151 & 153\end{bmatrix} + \begin{bmatrix}18 & 4\\ 6 & 14\end{bmatrix} = \begin{bmatrix}165 & 153\\ 157 & 167\end{bmatrix} \bmod 26 = \begin{bmatrix}9 & 7\\ 1 & 11\end{bmatrix} = e_2.$

$$(K + p_3) \bmod 26 = \begin{bmatrix} 147 & 149 \\ 151 & 153 \end{bmatrix} + \begin{bmatrix} 19 & 14 \\ 3 & 0 \end{bmatrix} = \begin{bmatrix} 166 & 163 \\ 154 & 153 \end{bmatrix} = \begin{bmatrix} 10 & 7 \\ 24 & 23 \end{bmatrix} \bmod 26 = e_3.$$

$$(K + p_4) \bmod 26 = \begin{bmatrix} 147 & 149 \\ 151 & 153 \end{bmatrix} + \begin{bmatrix} 24 & 1 \\ 17 & 14 \end{bmatrix} = \begin{bmatrix} 171 & 150 \\ 168 & 167 \end{bmatrix} \bmod 26 = \begin{bmatrix} 15 & 20 \\ 12 & 11 \end{bmatrix} =$$

e_4.

7. Finally, after converting $e_1, e_2, \ldots, e_6$ into the character, Alice have a ready chipper text to be sent: GEZXJHBLKHYXPUML.

Description Process

After receiving the message from Alice, Bob must do some steps to read the message as below:

1. Divide the message into 4-blocks as follows GEZX-JHBL-KHYX-PUML.
2. Convert the message into matrices :

$$\begin{bmatrix} 6 & 4 \\ 25 & 23 \end{bmatrix}; \begin{bmatrix} 9 & 7 \\ 1 & 11 \end{bmatrix}; \begin{bmatrix} 10 & 7 \\ 24 & 23 \end{bmatrix}; \begin{bmatrix} 15 & 20 \\ 12 & 11 \end{bmatrix}$$

3. Using secret key (K), Bob can read the message as below:

$$P1 = \left(\begin{bmatrix} 6 & 4 \\ 25 & 23 \end{bmatrix} - K \right) \bmod 26 = \begin{bmatrix} 15 & 11 \\ 4 & 0 \end{bmatrix};$$

$$P2 = \left(\begin{bmatrix} 9 & 7 \\ 1 & 11 \end{bmatrix} - K \right) \bmod 26 = \begin{bmatrix} 18 & 4 \\ 6 & 14 \end{bmatrix};$$

$$P3 = \left(\begin{bmatrix} 10 & 7 \\ 24 & 23 \end{bmatrix} - K \right) \bmod 26 = \begin{bmatrix} 19 & 14 \\ 3 & 0 \end{bmatrix};$$

$$P4 = \left(\begin{bmatrix} 15 & 20 \\ 12 & 11 \end{bmatrix} - K \right) \bmod 26 = \begin{bmatrix} 24 & 1 \\ 17 & 14 \end{bmatrix}.$$

4. Finally, Bob get the original message : PLEASE GO TODAY BRO

CONCLUSION

In this paper, we discuss the possibility of applying the concept of matrix multiplication for key exchange protocol based on Stickel's Algorithm. Nevertheless, we do not discuss the result for other aspect such as computation aspect related to complexity. Finally, we hope this idea can be applied in practical used in cryptography.

REFERENCE

[1] Myasnikov Alexei, Vladimir Shpilrain and Alexander Ushakov. 2008. *Group-based Cryptography*. Basel Switzerland: Birkhauser Verlag.

[2] Grigoriev,D and Vladimir S.. *Tropical Crypthography*. Downloaded at 12th April 2013.

[3] Stieckel. A New Public-Key Cryptosystem In Nonabelian Groups. Downloaded at 12th April 2014.

[4]Musthofa, Dwi Lestari. *The Password Agreement Method Based on Matrix Operation Over Min Plus Algebra for Secret Information safety* .2013.

[5] Bacelli, F., *et al*. *Synchronization and Linearity*. New York: John Wiley & Sons. 2001.